REMARKS

Claim 21 is amended and Claim 31 is added. Claims 21-31, as amended, remain in the application. No new matter is added by the amendments to the claims.

The Rejections:

In the Office Action dated February 28, 2006, the Examiner rejected Claims 21, 24-27, and 29 under 35 U.S.C. 102(b) as being anticipated by McNab, et al. (US 4,937,855).

As per Claim 21, the Examiner stated:

Method of initiating a procedure within a building comprising the steps of:

a. defining at least one initiating event for the procedure; [col.3, lines 23-31]

b. defining at least one requirement for the procedure; [col.9, lines 30-60]

c. defining at least one person to be authorized to perform the procedure; [col.8, lines 65-66]

d. detecting the at least one initiating event; [col.9, lines 30-60]

e. generating a virtual key for the at least one based on the at least one requirement detecting the at least one initiating event; [col.8, lines 33-34]

f. transmitting virtual key to the at least one person; [col.8, lines 43-47]

g. detecting use of the virtual key; [col.8, lines 32-34]

h. checking the validity of the virtual key; and [col.10, lines 28-44]

i. initiating said procedure within the building if the validity check is positive. [col.8, lines 36-40]

As per Claim 24, the Examiner stated: See col.3, lines 23-31; discusses defining different procedures for different initiating events.

As per Claim 25, the Examiner stated: See col.9, lines 30-60; discusses defining different requirements for different procedures.

As per Claim 26, the Examiner stated: See col.9, lines 30-60; discusses transmitting different virtual keys to said person for different initiating events.

As per Claim 27, the Examiner stated: See col.8, lines 32-34; discusses storing said virtual key partially or completely.

As per Claim 29, the Examiner stated:

method according to Claim 11, further comprising at least one of the steps of: initiating a control procedure of an elevator in the building; [col.9, lines 22-26] initiating a medical assistance procedure; [col.3, lines 25-29]

initiating a building cleaning procedure; and initiating a guest reception procedure. [col.9, lines 30-40]

The Examiner rejected Claims 22-23, 28, and 30 under 35 U.S.C. 103(a) as being unpatentable over McNab and in view of Microsoft Computer Dictionary, 5th Edition.

As per Claim 22, the Examiner stated:

McNab teaches authorized persons having access to the building according to a virtual key in the form of a code or a password. McNab did not fully disclose assigning an encrypted code to said virtual key. However, according to the Microsoft Computer Dictionary, encryption is the process of encoding data to prevent unauthorized access (page 192). Thus, it is obvious of ordinary skills in the art for the virtual key to be encrypted is an added security feature that further prevents any unauthorized persons from obtaining access any easier.

As per Claim 23, the Examiner stated:

McNab teaches authorized persons having access to the building according to a virtual key in the form of a code or a password. McNab did not include adding a signature to said virtual key and identifying a recipient of said transmitted virtual key by means of said signature. According to the Microsoft Computer Dictionary, a signature is a sequence of data used for identification for authentication purposes (page 480) and that a signature is also considered as a biometric technique (pages 59-60). By adding a signature to anything (i.e. virtual key, file, document) in the computer security related industry is known to protect sending the original file or key from being modified during transmission to another destination, thus, the signature of a virtual key is obviously for making sure the key is safe to use and have not been tampered with. Therefore, it would have been obvious for a person of ordinary skills in the art to include a signature to the virtual key of McNabb, is an added authentication feature and helps identify authorized persons from unidentified or unauthorized persons from being able to gain access to the building.

As per Claim 28, the Examiner stated:

McNab teaches authorized persons having access to the building according to a virtual key in the form of a code or a password. McNab did not include identifying said person with biometric characteristics. However, according to the Microsoft Computer Dictionary, biometric characteristics is a science of measuring and analyzing human biological characteristics wherein the computer technology this relates to authentication and security techniques (pages 59-60). It would have been obvious for a person of ordinary skills in the art to include biometric characteristics is a known authentication and security feature that is the actual (authorized) person's feature (i.e. fingerprint, retinal, signature) that is more complex to duplicate or hack for any unidentified persons to gain access to the building.

As per Claim 30, the Examiner stated:

McNab teaches authorized persons having access to the building remotely according to a virtual key in the form of a code or a password but did not include transmitting said virtual key using wireless devices. According to the Microsoft Computer Dictionary, the wireless communication feature takes place without use of wires or cables. Thus, it would have been obvious for a person of ordinary skills in the art to include wireless devices would be the conveniences of accessibility.

Applicants' Response:

The Examiner rejected Claims 22-23, 28, and 30 under 35 U.S.C. 103(a) as being unpatentable over McNab and in view of Microsoft Computer Dictionary, 5th Edition. However, the Microsoft Computer Dictionary has a 2002 copyright date identifying 2002 as the year of publication. Applicants' filing date is May 14, 2001 and Applicants claim a priority date of May 25, 2000. Thus, the Microsoft Computer Dictionary is not prior art and the rejection of Claims 22-23, 28, and 30 under 35 U.S.C. 103(a) is not proper.

The Examiner responded to Applicant's arguments filed September 19, 2005 as follows:

> "The claimed invention broadly states "defining at least one initiating event", is merely to identify what kind of person is to gain access to the building or a particular part within the building. Defining at least one initiating event as disclosed by McNabb is identifying the types of persons (i.e. visitor, guard, or postman) for the procedure which is to have access to a certain location or certain floor via the elevator in the building (col.9, lines 22-27) and then defining the requirements for that particular person that is deemed authorized and generates a

> virtual key base upon the requirement. McNabb discusses setting to operate in three different security levels pertaining to certain codes for either an apartment or a building (col.9, lines 30-55) and when the virtual key (or code) is generated for the visitor to use in order to gain access to the building (col.8, lines 13-67). McNabb discloses setting parameters for apartment security codes, a security level code, a guard security, a postman code, or a building code is the requirement for the procedure (col.8, lines 65-67). For instance, it is inherent a postman only needs access where the mailboxes are of a building so a postman is given the code or key that was set for the him to access a certain building and only go into the main floor where the mailboxes are and not else where of the building whereas the guard inherently is necessary for him to travel floor to floor and to all the building he is guarding. So the postman's requirements does not have to go door to door on every floor like the security guard. This concludes that the code is given after identifying the person prior to accessing certain locations (initiating event for the procedure) because it is necessary to identify the person in order to set and give the proper code to a particular location."

Applicants amended Claim 21 to clarify the steps d. and e. involve the detection of the occurrence of the at least one initiating event. Applicants added independent Claim 31 which adds security and availability requirements to the subject matter of Claim 21. (See Page 3, Lines 26-31)

The method according to the present invention generates a virtual key in response to the detection of the occurrence of a certain event. (Page 2, Lines 22-23) The person to whom the key is communicated is made to depend on the type of event. (Page 3, Lines 1-2) The event can be an emergency call, an order, a request such as for a cleaning service, an invitation, or a periodically recurring event such as, for example, monitoring a condition, or a service. (Page 3, Lines 23-25) The type of event determines what requirements are specified for the key such as security and availability. (Page 3, Lines 26 to Page 4, Line 3)

It is through the event that the person to be authorized is defined. (Page 4, Line 5) The person is defined in a processing step "Specify Person to be Authorized" **13**. (Page 4, Lines 8-9) As shown in the drawing of the flowchart for the method according to the present invention, the event occurs at the starting point **11** which is before the step **13** of specifying the person to be authorized.

The McNab et al. patent concerns a building security system for communication between building dwellers and visitors at an intercom station near the building entry (col. 2, lines 27-37).

McNab et al. also discusses rapid emergency communication and building access for selected personnel based on security codes (col. 3, lines 22-28). McNab et al. does not show or suggest the transmission of the security code to dwellers, visitors or selected personnel. In col.8, lines 32-40, McNab et al. states only that the security codes are preset and stored in a memory.

The Examiner equates Claim 21 step a. "defining at least one initiating event for the procedure" to the McNab building security system that provides access to selected personnel in response to the entry of a security code [col.3, lines 23-31]. The Examiner equates Claim 21 step b. "defining at least one requirement for the procedure" to the McNab security levels [col.9, lines 30-60]. The Examiner equates Claim 21 step c. "defining at least one person to be authorized to perform the procedure" to the McNab apartment security codes, a guard security or a postman code [col.8, lines 65-66]. The Examiner equates Claim 21 step d. "detecting the at least one initiating event" with the McNab entry of security codes into the security system [col.9, lines 30-60].

The Examiner has identified the "initiating event" as both the identification of the type of person (step a.) and the entry of the security code (step d.). However, the Examiner has overlooked a critical difference between the McNab security system and Applicants' method as defined by Claim 1. Applicants' virtual key (security code) is generated in step e. upon detecting the occurrence of the at least one initiating event and is transmitted to the at least one person in step f. Therefore the entry of the McNab security code cannot be the "initiating event" since such a security code would not be generated and transmitted to the person until the "initiating event" is detected.

The Examiner equates Claim 21 step e. "generating a virtual key for the at least one person based on the at least one requirement upon detecting the at least one initiating event" to the use of the security entry code by selected personnel in the McNab security system [col.8, lines 33-34]. The use of the McNab security code does not generate a virtual key based upon a requirement for the procedure and detection of the occurrence of the initiating event.

The Examiner equates Claim 21 step f. "transmitting virtual key to the at least one person" to the McNab remote programming of the system [col.8, lines 43-47]. This portion of the McNab patent describes changing the security codes in the system through remote access and has nothing to do with transmitting a virtual key to a person.

Thus, Claims 21-31 define a method in which the virtual key is generated only when the initiating event occurs and is detected. Only then is the virtual key generated and transmitted to an authorized person. In the McNab et al. security system, the security codes are preset and stored before an initiating event occurs. See the discussion cited by the Examiner (col. 8, lines 32-34) wherein the preset security code is entered at the panel keypad.

Therefore, Claims 21-31 define a method whereby an authorized person can only access a building if the initiating event has indeed occurred. Examples, of such initiating events are set forth on page 3 of Applicants' specification at lines 23-25. In the McNab et al. security system, the preset security codes are generated and stored before any event occurs and can be used to enter the building even if the associated event has not occurred.

The Examiner made of record but did not discuss references to Guertin, Pagel et al., Adams et al., Morearty and Freeny, Jr. Applicants reviewed these references and found them to be no more pertinent than the prior art relied upon by the Examiner in the rejections.

In view of the amendments to the claims and the above arguments, Applicants believe that the claims of record now define patentable subject matter over the art of record. Accordingly, an early Notice of Allowance is respectfully requested.